

Storing and accessing data in a mobile device and a user module

Patent number: DE10159398
Publication date: 2003-06-12
Inventor: KIRSCH JOCHEN (DE); KLAASSEN RALF (DE)
Applicant: GIESECKE & DEVRIENT GMBH (DE)
Classification:
- **International:** H04M1/247; H04L9/30; H04Q7/32
- **European:** H04Q7/32A6
Application number: DE20011059398 20011204
Priority number(s): DE20011059398 20011204

Also published as:
 WO03049471 (A1)
 EP1454503 (A1)
 US2005120225 (A1)

Report a data error here

Abstract of DE10159398

The invention relates to a method for storing and accessing useful data (48) and configuration data (62) in a mobile device (10) that is linked with a user module (12). According to a first embodiment of the invention, the at least part of the useful data (48) is stored in the mobile device (10) in encrypted form and, when the data is accessed, decrypted using a decryption function (66) of the user module (12). According to a second embodiment of the invention, the configuration data (62) is stored in the user module (12). The configuration data (62) indicates whether and to what extent an application program (46) may be executed by the mobile device (10). The invention increases security of useful data (48) and application programs (46) in the mobile device (10) and protection against unauthorized access thereto.

Data supplied from the **esp@cenet** database - Worldwide

This Page Blank (reverse)

⑩ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

⑫ Offenlegungsschrift
⑩ DE 101 59 398 A 1

⑤ Int. Cl. 7:
H 04 M 1/247
H 04 L 9/30
H 04 Q 7/32

⑪ Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

⑫ Erfinder:
Kirsch, Jochen, 80797 München, DE; Klaassen, Ralf, 81825 München, DE

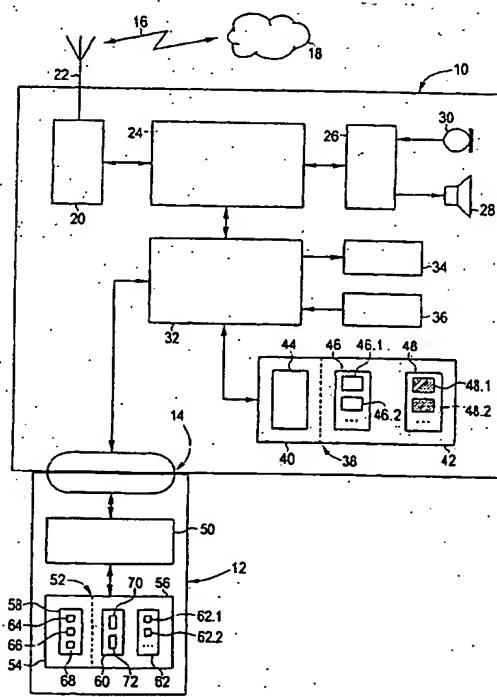
⑯ Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 197 41 330 A1
DE 197 24 901 A1
DE 195 24 773 A1
DE 100 17 424 A1
EP 12 21 691 A1
WO 91 12 698 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

⑮ Speichern von und Zugreifen auf Daten in einem Mobilgerät und einem Benutzermodul

⑯ Die Erfindung betrifft Verfahren zum Speichern von und Zugreifen auf Nutzdaten (48) und Konfigurationsdaten (62) in einem Mobilgerät (10), das mit einem Benutzermodul (12) verbunden ist. Nach einem ersten Aspekt der Erfindung werden die Nutzdaten (48) im Mobilgerät (10) zumindest teilweise in verschlüsselter Form gespeichert und bei Zugriffsvorgängen unter Verwendung einer Entschlüsselungsfunktion (66) des Benutzermoduls (12) entschlüsselt. Nach einem zweiten Aspekt der Erfindung werden die Konfigurationsdaten (62) im Benutzermodul (12) gespeichert. Die Konfigurationsdaten (62) geben an, ob bzw. in welchem Umfang ein Anwendungsprogramm (46) von dem Mobilgerät (10) ausgeführt werden darf. Durch die Erfindung werden die Sicherheit und der Schutz gegen unberechtigte Zugriffe auf Nutzdaten (48) und Anwendungsprogramme (46) in dem Mobilgerät (10) erhöht.



Beschreibung

[0001] Die Erfindung betrifft allgemein das technische Gebiet des Speicherns von und Zugreifens auf Daten in Mobilgeräten sowie in Benutzermodulen für derartige Geräte. Ein bevorzugtes Einsatzgebiet der Erfindung sind Mobilgeräte, die dem Benutzer sowohl Telekommunikationsfunktionen (z. B. die Sprach- und/ oder Datenübertragung über ein Telekommunikationsnetz) als auch Anwendungsprogramme (z. B. einen Terminplaner oder einen Texteditor) bereitstellen. Derartige Mobilgeräte können insbesondere als leistungsfähige Mobiltelefone oder als persönliche digitale Assistenten (PDAs = personal digital assistants) ausgestaltet sein.

[0002] Die deutsche Offenlegungsschrift DE 197 24 901 A1 zeigt ein Mobiltelefon nach dem GSM-Standard (GSM = global system for mobile communication). Das Mobiltelefon weist eine Steuerinheit, einen Gerätespeicher und eine Schnittstelle für ein Teilnehmeridentifikationsmodul (SIM = subscriber identity module) auf. Über eine Leitungsverbindung mit einem Computer können Nutzdaten, z. B. Adressenlisten oder Umsatzdaten oder Preislisten, in den Gerätespeicher geladen werden. Ferner ist die Möglichkeit vorgesehen, über die Leitungsverbindung nicht näher spezifizierte Programme in den Gerätespeicher zu laden und später durch das Mobiltelefon ausführen zu lassen. Die Datenübertragung kann integritätsgeichert oder verschlüsselt erfolgen.

[0003] In der Regel wird beim Einschalten eines GSM-Mobiltelefons eine Berechtigungsabfrage durchgeführt, bei der der Benutzer eine persönliche Geheimzahl (PIN = personal identification number) eingeben muss. Die vollständige Benutzeroberfläche einschließlich der Zugriffsmöglichkeit auf die in dem Mobiltelefon gespeicherten Nutzdaten wird nur bei korrekter Eingabe der Geheimzahl freigegeben. Die meist vertraulichen Nutzdaten sind damit in gewissem Umfang gesichert. Es besteht jedoch das Problem, dass diese Sicherung mit hinreichender krimineller Energie umgangen werden kann. So können beispielsweise mittels geeigneter Geräte Speicherbausteine des Mobiltelefons unmittelbar auf Hardwareebene ausgelesen werden.

[0004] Die Speicherung von Nutzdaten im Mobilgerät ist insbesondere dann sinnvoll, wenn das Mobilgerät auch zum Ausführen von Anwendungsprogrammen zur Verarbeitung dieser Nutzdaten eingerichtet ist. Diese Funktionalität ist heute schon bei leistungsfähigen GSM-Mobiltelefonen sowie bei PDAs gegeben. Für Mobilgeräte der 2.5-ten und 3-ten Generation, z. B. Geräte für die Netze GPRS (general packet radio service), EDGE, UMTS (universal mobile telecommunications system) und WCDMA (wideband code-division multiple access) ist es wegen der hohen Übertragungsgeschwindigkeiten realistisch, Anwendungsprogramme über die Luftschaltungstelle von einem Dienstanbieter in das Mobilgerät zu laden und/oder zu aktualisieren.

[0005] Bei den genannten Mobilgeräten bestehen Probleme beziehungsweise Verbesserungsbedarf in mehrreli Hinsicht. Erstens soll auch hier ein unautorisierte Zugriff auf Anwendungsprogramme verhindert werden. Es soll also sichergestellt sein, dass nur der berechtigte Benutzer ein Anwendungsprogramm beziehungsweise einzelne gesicherte Funktionen des Anwendungsprogramms aufrufen kann. Zweitens wäre eine Möglichkeit wünschenswert, dem Benutzer eine möglichst genau auf seine Bedürfnisse zugeschnittene Auswahl von Funktionen anzubieten. Drittens soll eine möglichst weitgehende Gerätunabhängigkeit der bereitgestellten Funktionen erreicht werden.

[0006] Die Erfindung hat die Aufgabe, die genannten Probleme ganz oder teilweise zu lösen. Insbesondere sollen

durch die Erfindung die Sicherheit und der Schutz gegen unberechtigte Zugriffe auf Nutzdaten und Anwendungsprogramme in einem Mobilgerät erhöht werden. In bevorzugten Ausgestaltungen soll die Erfindung ferner hohen Komfort für den Benutzer bereitstellen und kostengünstig verwirklicht werden können.

[0007] Erfindungsgemäß wird diese Aufgabe ganz oder zum Teil gelöst durch ein Verfahren mit den Merkmalen der Ansprüche 1 beziehungsweise 10, ein Mobilgerät mit den Merkmalen der Ansprüche 8 beziehungsweise 17 und ein Benutzermodul mit den Merkmalen der Ansprüche 9 beziehungsweise 19. Die abhängigen Ansprüche betreffen bevorzugte Ausgestaltungen der Erfindung.

[0008] Die Erfindung geht von der Grundidee aus, durch eine geeignete Speicherung der Nutz- beziehungsweise Konfigurationsdaten die oben genannten Sicherheitsanforderungen zu erfüllen.

[0009] Ein erster Aspekt der Erfindung betrifft das Speichern der Nutzdaten. Diese werden erfindungsgemäß im Gerätespeicher des Mobilgeräts in verschlüsselter Form abgelegt. Zumindest zum Entschlüsseln der Nutzdaten (und in bevorzugten Ausgestaltungen auch zum Verschlüsseln) dienen entsprechende Funktionen, die vom Benutzermodul bereitgestellt werden.

[0010] Dadurch, dass die Nutzdaten im Speicher des Mobilgeräts lediglich in verschlüsselter Form vorliegen, sind diese Daten auch dann gegen Ausspähung gesichert, wenn sich ein Unbefugter unter Umgehung der normalen Benutzeroberfläche des Mobilgeräts Zugriff auf den Inhalt des Gerätespeichers verschafft. Der in der Regel großzügig bemessene Gerätespeicher kann ohne Sicherheitsbedenken zur Speicherung der Nutzdaten eingesetzt werden, wodurch sich größere Datenmengen und komplexe Datenstrukturen im Mobilgerät mitführen lassen.

[0011] Die erfindungsgemäß zur Speicherung vorgesehenen Nutzdaten können beliebige vom Benutzer gewünschte Daten sein. Vorzugsweise sind dies Daten, die auch von einem auf dem Mobilgerät laufenden Anwendungsprogramm verarbeitet werden können, beispielsweise Termin- und Adressenlisten zur Verarbeitung durch einen Terminplaner mit Adressbuchfunktion, geschäftliche Tabellen z. B. zur Verarbeitung durch Tabellenkalkulationsprogramme, Sprachdaten beispielsweise erzeugt durch Diktataufzeichnungsprogramme oder allgemeine Texte zur Verarbeitung durch Texteditoren. Auch eine Speicherung von Nutzdaten, für die kein entsprechendes Anwendungsprogramm im Mobilgerät verfügbar ist, kann wünschenswert sein. Das Mobilgerät dient dann als sicherer Datenträger zum Austausch der Nutzdaten z. B. zwischen dem Arbeitsplatz und einem Heimbüro.

[0012] In bevorzugten Ausgestaltungen werden die Ver- und Entschlüsselungsfunktionen teilweise oder vollständig von einer Prozessoreinheit des Benutzermoduls ausgeführt, wobei die Prozessoreinheit auf Schlüsseldaten zugreift, die in einem Modulspeicher enthalten sind. Die Schlüsseldaten brauchen in diesen Ausgestaltungen das Benutzermodul nicht zu verlassen, wodurch eine besonders hohe Sicherheit erzielt wird. Dies gilt besonders dann, wenn die Schlüsseldaten auch innerhalb des Benutzermoduls erzeugt und in den Modulspeicher eingeschrieben werden. Es sind jedoch auch Ausgestaltungen der Erfindung vorgesehen, bei denen zumindest das Verschlüsseln und möglicherweise auch das Entschlüsseln der Nutzdaten ganz oder teilweise durch eine Prozessoreinheit des Mobilgeräts ausgeführt wird, an die die vom Benutzermodul bereitgestellten Ver- und/ oder Entschlüsselungsfunktionen übertragen werden.

[0013] Vorzugsweise wird ein asymmetrisches Verschlüsselungsverfahren wie z. B. das RSA-Verfahren (RSA = Ri-

vest-Shamir-Adleman) eingesetzt. Die Schlüsseldaten weisen dann einen öffentlichen Schlüssel und einen privaten Schlüssel auf. Es sind jedoch auch Ausgestaltungen vorgesehen, bei denen symmetrische Verschlüsselungsverfahren verwendet werden. Konzeptuell wird auch bei diesen Ausgestaltungen von "Ver- und Entschlüsselungsfunktionen" gesprochen, auch wenn in beiden Fällen die gleichen Berechnungsschritte ausgeführt werden.

[0014] Erfindungsgemäß ist zumindest zum Ausführen der Entschlüsselungsschritte das Benutzermodul erforderlich. Dies bewirkt bereits einen gewissen Schutz, weil das Benutzermodul und das Mobilgerät getrennt aufbewahrt werden können. In bevorzugten Ausführungsformen ist jedoch vorgesehen, dass zumindest die Entschlüsselungsfunktion nur nach Eingabe eines Kennworts (passphrase) und/oder nach einer biometrischen Prüfung, z. B. der Prüfung eines Fingerabdrucks oder einer Sprachanalyse, freigegeben wird. Durch diese Maßnahme ist die Datensicherheit auch dann gewährleistet, wenn das Mobilgerät zusammen mit dem Benutzermodul abhanden kommt.

[0015] Ein zweiter Aspekt der Erfindung betrifft die Verwendung von Konfigurationsdaten beim Ausführen eines Anwendungsprogramms in dem Mobilgerät. Dieser Aspekt beruht auf der Grundidee, durch die Konfigurationsdaten die Verfügbarkeit des gesamten Anwendungsprogramms oder einzelner Funktionen des Anwendungsprogramms anzugeben. Die Konfigurationsdaten werden im Benutzermodul gespeichert, während das Anwendungsprogramm im Mobilgerät vorliegt. Das Anwendungsprogramm wird nur dann bzw. nur in dem Umfang ausgeführt, wie dies durch die Konfigurationsdaten angegeben ist.

[0016] Die erfundungsgemäße Lehre bietet Schutz gegen eine unautorisierte Ausführung des Anwendungsprogramms bzw. einzelner Programmfunctionen, da neben dem Mobilgerät stets auch das Benutzermodul mit den entsprechenden, die Programmausführung zulassenden Konfigurationsdaten erforderlich ist. Ferner schafft die Erfindung die technischen Grundlagen, um eine genau auf die Bedürfnisse des Benutzers zugeschnittene Programmkonfiguration bereitzustellen. Dies ist insbesondere dann von Bedeutung, wenn für die Programmbenutzung ein von der zur Verfügung gestellten Funktionalität abhängiges Entgelt zu entrichten ist, wie dies beispielsweise bei ASP-Angeboten (ASP = application service providing) der Fall ist. Da erfundungsgemäß die Konfigurationsdaten im Benutzermodul gespeichert sind, kann der Benutzer durch einfaches Umstecken des Benutzermoduls die von ihm gewünschte Konfiguration bei beliebigen kompatiblen Mobilgeräten einstellen.

[0017] Unter dem hier verwendeten Begriff "Anwendungsprogramm" sind insbesondere Programme zu verstehen, die Datenverarbeitungsfunktionen hinsichtlich der oben genannten Nutzdaten ausführen. Wenn es sich bei dem Mobilgerät um ein Gerät mit Telekommunikationsfunktionen handelt, sind die Anwendungsprogramme vorzugsweise unabhängig von diesen Telekommunikationsfunktionen oder zumindest auch für andere Zwecke nutzbar. Beispiele typischer Anwendungsprogramme sind Terminplaner, Adressbücher, Texteditoren, Tabellenkalkulationsprogramme, Datenbanken, Diktataufzeichnungsprogramme und so weiter. Auch Programme, die nur Benutzeroberflächen für die oben genannten oder ähnliche Anwendungen bereitstellen (während die eigentlichen Datenverarbeitungsvorgänge durch den Server eines ASP-Anbieters ausgeführt werden), sollen im hier verwendeten Sinne als Anwendungsprogramme aufgefasst werden. In manchen Ausgestaltungen sind auch Browser und Viewer zur formatierten Anzeige von Dokumenten als Anwendungsprogramme vorgesehen.

[0018] Zur weiteren Erhöhung des Schutzes gegen eine unberechtigte Ausführung der Anwendungsprogramme ist vorzugsweise das Auslesen der Konfigurationsdaten durch ein Kennwort und/oder eine biometrische Überprüfung, z. B. eine Stimm- oder Fingerabdruckanalyse, gesichert.

5 Das Benutzermodul gibt nur dann die Konfigurationsdaten frei und ermöglicht dadurch das Ausführen des entsprechenden Anwendungsprogramms beziehungsweise der entsprechenden Programmfunction, wenn sich der Benutzer durch das Kennwort und/oder seine biometrischen Daten hinreichend identifizieren konnte.

[0019] Die erfundungsgemäße Funktionalität ist auch bei Mobilgeräten einsetzbar, die ein oder mehrere fest gespeicherte Anwendungsprogramme enthalten. Vorzugsweise

15 dienen die Konfigurationsdaten jedoch auch dazu, das Laden von Anwendungsprogrammen oder zumindest Teilen davon in das Mobilgerät zu steuern. Insbesondere bei Mobilgeräten, die leistungsfähige Funktionen zur drahtlosen Datenübertragung aufweisen, können die Anwendungspro-

gramme oder die benötigten Programmmodulen über die Luftschnittstelle von einem externen Dienstanbieter geladen werden. Diese Möglichkeit ist im Zusammenhang mit ASP-Angeboten besonders vorteilhaft. Der Komfort für den Benutzer wird erheblich gesteigert, wenn er bereits durch die

25 bloße Verwendung des Benutzermoduls auf jedem kompatiblen Mobilgerät ein automatisches Laden der benötigten Anwendungsprogramme entsprechend seiner Konfiguration initiieren kann. Das herstellerunabhängige Laden von Anwendungsprogrammen wird durch die Verwendung von

30 Programmiersprachen unterstützt, die unabhängig von der Rechnerplattform arbeiten, wie dies beispielsweise auf Java® zutrifft.

[0020] Besonders vorteilhaft ist eine Verbindung der beiden genannten Aspekte der Erfindung, weil dadurch ein Schutz gegen unberechtigten Zugriff auf die Nutzdaten und ein Schutz gegen die unberechtigte Ausführung von Anwendungsprogrammen erreicht wird.

[0021] Das Mobilgerät ist in bevorzugten Ausgestaltungen beider oben genannten Aspekte ein Telekommunikationsgerät, insbesondere ein Mobiltelefon oder ein persönlicher digitaler Assistent (PDA) mit Telefoniefunktionen. Das Benutzermodul ist vorzugsweise ein Teilnehmeridentifikationsmodul (SIM = subscriber identification module), wie es auch zur Einbuchtung in ein Telekommunikationsnetz benötigt wird. Insbesondere kann ein Benutzermodul vorgesehen sein, das als sogenanntes trusted device oder tamper resistant device manipulationsgesichert ist, so dass ein Ausspähen der Ver- und Entschlüsselungsfunktionen oder der Schlüsseldaten oder vertraulicher Konfigurationsdaten verhindert wird.

40 Die Verwendung eines Teilnehmeridentifikationsmoduls bietet sich auch dann an, wenn das Mobilgerät keine Telefoniefunktionen aufweist oder das Modul nicht bei einem Telefonieanbieter registriert ist, weil derartige Module in großen Stückzahlen hergestellt werden und dadurch relativ kostengünstig verfügbar sind.

[0022] Das Mobilgerät und das Benutzermodul sind vorzugsweise mit Merkmalen weitergebildet, die den oben beschriebenen und/oder in den abhängigen Verfahrensansprüchen genannten Merkmalen entsprechen.

[0023] Weitere Merkmale, Vorteile und Aufgaben der Erfindung gehen aus der folgenden genauen Beschreibung eines Ausführungsbeispiels der Erfindung und mehrerer Ausführungsalternativen hervor. Es wird auf die schematische Zeichnung verwiesen, in der Fig. 1 ein Blockdiagramm wesentlicher Funktionseinheiten eines Systems nach dem vorliegend beschriebenen Ausführungsbeispiel der Erfindung zeigt.

[0024] In Fig. 1 sind ein Mobilgerät 10 und ein Benutzer-

modul 12 dargestellt, die über eine Schnittstelle 14 miteinander verbunden sind. Das Mobilgerät 10 ist im vorliegenden Ausführungsbeispiel als leistungsfähiges Mobiltelefon ausgestaltet, das Telekommunikationsfunktionen gemäß den Standards GSM für Telefoniedienste und GPRS für Datenübertragungsdienste bereitstellt. Entsprechend ist das Benutzermodul 12 als SIM-Karte ausgebildet, welche in das Mobiltelefon eingesetzt wird oder fest im Mobiltelefon angeordnet ist. Über eine Luftschnittstelle 16 vermag das Mobilgerät 10 auf ein entsprechendes Telekommunikationsnetz 18 zuzugreifen. In Ausführungsalternativen ist das Mobilgerät 10 nach einem weiterentwickelten Mobilfunkstandard, z. B. UMTS, und/oder als persönlicher digitaler Assistant (PDA) ausgestaltet.

[0025] In an sich bekannter Weise weist das Mobilgerät 10 einen Hochfrequenzteil 20 auf, der Funkwellen über eine Antenne 22 sendet und empfängt. Ein digitaler Signalprozessor (DSP) 24 dient zur Verarbeitung des Sendebzw. Empfangssignals. Ferner verarbeitet der digitale Signalprozessor 24 Niederfrequenzsignale, die über einen Niederfrequenzteil 26 an einen Lautsprecher 28 geleitet werden beziehungsweise von einem Mikrofon 30 über den Niederfrequenzteil 26 an den digitalen Signalprozessor 24 ausgegeben werden. Eine Prozessoreinheit 32 koordiniert alle im Mobilgerät 10 ablaufenden Vorgänge. Die Prozessoreinheit 32 ist mit der Schnittstelle 14, dem digitalen Signalprozessor 24, einer hier als grafikfähiges LCD-Display ausgestalteten Anzeige 34, einer Tastatur 36 und einem Gerätespeicher 38 verbunden. Der Gerätespeicher 38 kann fest installiert oder abnehmbar, beispielsweise in Form einer Speicherplatte, ausgeführt sein.

[0026] Der Gerätespeicher 38 ist durch mehrere Halbleiterchips in unterschiedlichen Speichertechnologien implementiert. In der konzeptionellen Darstellung von Fig. 1 weist der Gerätespeicher 38 einen nur-lesbaren Bereich 40 (z. B. implementiert als maskenprogrammiertes ROM) und einen beschreibbaren Bereich 42, z. B. implementiert als RAM oder EEPROM oder FLASH-Speicher, auf. Der nur-lesbare Bereich 40 des Gerätespeichers 38 enthält insbesondere Betriebssprogramme 44, die von der Prozessoreinheit 32 als grundlegendes Betriebssystem des Mobilgeräts 10 sowie zur Implementierung der Telekommunikationsfunktionen ausgeführt werden. In den beschreibbaren Bereich 42 sind Anwendungsprogramme 46 und Nutzdaten 48 geladen.

[0027] Fig. 1 zeigt als Beispiel für die Anwendungsprogramme 46 einen Terminplaner 46.1 (mit Adressbuchfunktion) und einen Texteditor 46.2. Als Nutzdaten 48 sind in Fig. 1 eine Termin- und Adressenliste 48.1 für den Terminplaner 46.1 und ein Brief 48.2 für den Texteditor 46.2 dargestellt. Die Anwendungsprogramme 46 werden von der Prozessoreinheit 32 ausgeführt und greifen auf die Nutzdaten 48 zu. Die Nutzdaten 48 sind im Gerätespeicher 38 verschlüsselt abgelegt, was in Fig. 1 durch eine Schraffur ange deutet ist.

[0028] Das Benutzermodul 12 ist als Teilnehmeridentifikationsmodul (SIM) für das Telekommunikationsnetz 18 ausgestaltet, und auch die Schnittstelle 14 entspricht mechanisch und elektrisch den für dieses Telekommunikationsnetz 18 vorgesehenen Normen. Das Benutzermodul 12 weist eine als Mikrocontroller ausgestaltete Prozessoreinheit 50 auf, die auf einem einzigen Chip mit einem Modulspeicher 52 integriert ist. Der Modulspeicher 52 ist durch unterschiedliche Speichertechnologien in einen nur-lesbaren Bereich 54 und einen beschreibbaren Bereich 56 unterteilt.

[0029] Der Modulspeicher 52 enthält Steuerprogramme und Daten, die erstens grundlegende Betriebssystemfunktionen für das Benutzermodul 12 bereitstellen und zweitens das Einbuchen und den Telekommunikationsbetrieb des

Mobilgeräts 10 im Hinblick auf das Telekommunikationsnetz 18 ermöglichen. Aus Gründen der Übersichtlichkeit sind diese Steuerprogramme und Daten in Fig. 1 nicht gesondert dargestellt. Für die erfindungsgemäßen Aspekte des hier beschriebenen Ausführungsbeispiels besonders relevant und deshalb in Fig. 1 gezeigt sind kryptographische Funktionen 58 im nur-lesbaren Bereich 54 des Modulspeichers 52 sowie Schlüsseldaten 60 und Konfigurationsdaten 62 im beschreibbaren Bereich 56.

10 [0030] Die kryptographischen Funktionen 58 enthalten eine Verschlüsselungsfunktion 64, eine Entschlüsselungsfunktion 66 und eine Schlüsselerzeugungsfunktion 68. Die Schlüsseldaten 60 teilen sich in einen öffentlichen Schlüssel 70 und einen privaten Schlüssel 72 auf. Die Konfigurationsdaten 62 weisen für jedes im Mobilgerät 10 vorgesehene Anwendungsprogramm 46 einen entsprechenden Konfigurationsdatensatz auf, nämlich im hier beschriebenen Ausführungsbeispiel einen Konfigurationsdatensatz 62.1 für den Terminplaner 46.1 sowie einen Konfigurationsdatensatz 62.2 für den Texteditor 46.2.

15 [0031] Im Betrieb stellt das in Fig. 1 gezeigte System die üblichen Telekommunikationsfunktionen entsprechend den jeweiligen Standards, im vorliegenden Fall GSM und GPRS, bereit. Zusätzlich kann der Benutzer die Anwendungsprogramme 46 aufrufen und mit diesen die Nutzdaten 48 oder andere Daten bearbeiten.

20 [0032] Zum Bereitstellen der Anwendungsprogramme 46 greift das Mobilgerät 10 beim Einschalten oder spätestens, wenn der Benutzer ein Anwendungsprogramm 46 starten möchte, auf die Konfigurationsdaten 62 im Benutzermodul 12 zu. Dieser Zugriff erfolgt über die Prozessoreinheit 50 des Benutzermoduls 12, die ihrerseits zunächst eine Kennworteingabe anfordert, bevor sie den Zugriff freigibt. Die Kennwortanforderung wird auf der Anzeige 34 des Mobilgeräts 10 angezeigt, und der Benutzer gibt das entsprechende Kennwort über die Tastatur 36 ein. Die Korrektheit des Kennworts wird durch die Prozessoreinheit 50 überprüft.

25 [0033] Hat der Benutzer das korrekte Kennwort eingegeben, so überträgt das Benutzermodul 12 die angeforderten Konfigurationsdaten 62 (entweder alle Konfigurationsdaten 62 oder nur den für das jeweilige Anwendungsprogramm 46.1, 46.2 vorgesehenen Datensatz 62.1, 62.2) an das Mobilgerät 10. Die Prozessoreinheit 32 überprüft nun, ob gemäß den übertragenen Konfigurationsdaten 62, 62.1, 62.2 die Ausführung von Anwendungsprogrammen 46 oder des konkret angeforderten Anwendungsprogramms 46.1, 46.2 zulässig ist. Ist dies der Fall, so wird die Programmausführung freigegeben.

30 [0034] Wenn sich das gewünschte Anwendungsprogramm 46.1, 46.2 bereits im Gerätespeicher 38 befindet, kann das Programm ohne weiteres gestartet werden. Andernfalls wird das benötigte Programm über die Luftschnittstelle 16 und das Telekommunikationsnetz 18 von einem Server eines ASP-Anbieters in den Gerätespeicher 38 geladen. Auch dieser Download-Vorgang muss durch das Benutzermodul 12 autorisiert werden, das hierbei als sogenannter gatekeeper arbeitet. Selbst wenn das gewünschte Anwendungsprogramm 46.1, 46.2 bereits im Gerätespeicher 38 enthalten ist,

35 45 55 60 65 70 75 80 85 90 95 100 105 110 115 120 125 130 135 140 145 150 155 160 165 170 175 180 185 190 195 200 205 210 215 220 225 230 235 240 245 250 255 260 265 270 275 280 285 290 295 300 305 310 315 320 325 330 335 340 345 350 355 360 365 370 375 380 385 390 395 400 405 410 415 420 425 430 435 440 445 450 455 460 465 470 475 480 485 490 495 500 505 510 515 520 525 530 535 540 545 550 555 560 565 570 575 580 585 590 595 600 605 610 615 620 625 630 635 640 645 650 655 660 665 670 675 680 685 690 695 700 705 710 715 720 725 730 735 740 745 750 755 760 765 770 775 780 785 790 795 800 805 810 815 820 825 830 835 840 845 850 855 860 865 870 875 880 885 890 895 900 905 910 915 920 925 930 935 940 945 950 955 960 965 970 975 980 985 990 995 1000 1005 1010 1015 1020 1025 1030 1035 1040 1045 1050 1055 1060 1065 1070 1075 1080 1085 1090 1095 1100 1105 1110 1115 1120 1125 1130 1135 1140 1145 1150 1155 1160 1165 1170 1175 1180 1185 1190 1195 1200 1205 1210 1215 1220 1225 1230 1235 1240 1245 1250 1255 1260 1265 1270 1275 1280 1285 1290 1295 1300 1305 1310 1315 1320 1325 1330 1335 1340 1345 1350 1355 1360 1365 1370 1375 1380 1385 1390 1395 1400 1405 1410 1415 1420 1425 1430 1435 1440 1445 1450 1455 1460 1465 1470 1475 1480 1485 1490 1495 1500 1505 1510 1515 1520 1525 1530 1535 1540 1545 1550 1555 1560 1565 1570 1575 1580 1585 1590 1595 1600 1605 1610 1615 1620 1625 1630 1635 1640 1645 1650 1655 1660 1665 1670 1675 1680 1685 1690 1695 1700 1705 1710 1715 1720 1725 1730 1735 1740 1745 1750 1755 1760 1765 1770 1775 1780 1785 1790 1795 1800 1805 1810 1815 1820 1825 1830 1835 1840 1845 1850 1855 1860 1865 1870 1875 1880 1885 1890 1895 1900 1905 1910 1915 1920 1925 1930 1935 1940 1945 1950 1955 1960 1965 1970 1975 1980 1985 1990 1995 2000 2005 2010 2015 2020 2025 2030 2035 2040 2045 2050 2055 2060 2065 2070 2075 2080 2085 2090 2095 2100 2105 2110 2115 2120 2125 2130 2135 2140 2145 2150 2155 2160 2165 2170 2175 2180 2185 2190 2195 2200 2205 2210 2215 2220 2225 2230 2235 2240 2245 2250 2255 2260 2265 2270 2275 2280 2285 2290 2295 2300 2305 2310 2315 2320 2325 2330 2335 2340 2345 2350 2355 2360 2365 2370 2375 2380 2385 2390 2395 2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490 2495 2500 2505 2510 2515 2520 2525 2530 2535 2540 2545 2550 2555 2560 2565 2570 2575 2580 2585 2590 2595 2600 2605 2610 2615 2620 2625 2630 2635 2640 2645 2650 2655 2660 2665 2670 2675 2680 2685 2690 2695 2700 2705 2710 2715 2720 2725 2730 2735 2740 2745 2750 2755 2760 2765 2770 2775 2780 2785 2790 2795 2800 2805 2810 2815 2820 2825 2830 2835 2840 2845 2850 2855 2860 2865 2870 2875 2880 2885 2890 2895 2900 2905 2910 2915 2920 2925 2930 2935 2940 2945 2950 2955 2960 2965 2970 2975 2980 2985 2990 2995 3000 3005 3010 3015 3020 3025 3030 3035 3040 3045 3050 3055 3060 3065 3070 3075 3080 3085 3090 3095 3100 3105 3110 3115 3120 3125 3130 3135 3140 3145 3150 3155 3160 3165 3170 3175 3180 3185 3190 3195 3200 3205 3210 3215 3220 3225 3230 3235 3240 3245 3250 3255 3260 3265 3270 3275 3280 3285 3290 3295 3300 3305 3310 3315 3320 3325 3330 3335 3340 3345 3350 3355 3360 3365 3370 3375 3380 3385 3390 3395 3400 3405 3410 3415 3420 3425 3430 3435 3440 3445 3450 3455 3460 3465 3470 3475 3480 3485 3490 3495 3500 3505 3510 3515 3520 3525 3530 3535 3540 3545 3550 3555 3560 3565 3570 3575 3580 3585 3590 3595 3600 3605 3610 3615 3620 3625 3630 3635 3640 3645 3650 3655 3660 3665 3670 3675 3680 3685 3690 3695 3700 3705 3710 3715 3720 3725 3730 3735 3740 3745 3750 3755 3760 3765 3770 3775 3780 3785 3790 3795 3800 3805 3810 3815 3820 3825 3830 3835 3840 3845 3850 3855 3860 3865 3870 3875 3880 3885 3890 3895 3900 3905 3910 3915 3920 3925 3930 3935 3940 3945 3950 3955 3960 3965 3970 3975 3980 3985 3990 3995 4000 4005 4010 4015 4020 4025 4030 4035 4040 4045 4050 4055 4060 4065 4070 4075 4080 4085 4090 4095 4100 4105 4110 4115 4120 4125 4130 4135 4140 4145 4150 4155 4160 4165 4170 4175 4180 4185 4190 4195 4200 4205 4210 4215 4220 4225 4230 4235 4240 4245 4250 4255 4260 4265 4270 4275 4280 4285 4290 4295 4300 4305 4310 4315 4320 4325 4330 4335 4340 4345 4350 4355 4360 4365 4370 4375 4380 4385 4390 4395 4400 4405 4410 4415 4420 4425 4430 4435 4440 4445 4450 4455 4460 4465 4470 4475 4480 4485 4490 4495 4500 4505 4510 4515 4520 4525 4530 4535 4540 4545 4550 4555 4560 4565 4570 4575 4580 4585 4590 4595 4600 4605 4610 4615 4620 4625 4630 4635 4640 4645 4650 4655 4660 4665 4670 4675 4680 4685 4690 4695 4700 4705 4710 4715 4720 4725 4730 4735 4740 4745 4750 4755 4760 4765 4770 4775 4780 4785 4790 4795 4800 4805 4810 4815 4820 4825 4830 4835 4840 4845 4850 4855 4860 4865 4870 4875 4880 4885 4890 4895 4900 4905 4910 4915 4920 4925 4930 4935 4940 4945 4950 4955 4960 4965 4970 4975 4980 4985 4990 4995 5000 5005 5010 5015 5020 5025 5030 5035 5040 5045 5050 5055 5060 5065 5070 5075 5080 5085 5090 5095 5100 5105 5110 5115 5120 5125 5130 5135 5140 5145 5150 5155 5160 5165 5170 5175 5180 5185 5190 5195 5200 5205 5210 5215 5220 5225 5230 5235 5240 5245 5250 5255 5260 5265 5270 5275 5280 5285 5290 5295 5300 5305 5310 5315 5320 5325 5330 5335 5340 5345 5350 5355 5360 5365 5370 5375 5380 5385 5390 5395 5400 5405 5410 5415 5420 5425 5430 5435 5440 5445 5450 5455 5460 5465 5470 5475 5480 5485 5490 5495 5500 5505 5510 5515 5520 5525 5530 5535 5540 5545 5550 5555 5560 5565 5570 5575 5580 5585 5590 5595 5600 5605 5610 5615 5620 5625 5630 5635 5640 5645 5650 5655 5660 5665 5670 5675 5680 5685 5690 5695 5700 5705 5710 5715 5720 5725 5730 5735 5740 5745 5750 5755 5760 5765 5770 5775 5780 5785 5790 5795 5800 5805 5810 5815 5820 5825 5830 5835 5840 5845 5850 5855 5860 5865 5870 5875 5880 5885 5890 5895 5900 5905 5910 5915 5920 5925 5930 5935 5940 5945 5950 5955 5960 5965 5970 5975 5980 5985 5990 5995 6000 6005 6010 6015 6020 6025 6030 6035 6040 6045 6050 6055 6060 6065 6070 6075 6080 6085 6090 6095 6100 6105 6110 6115 6120 6125 6130 6135 6140 6145 6150 6155 6160 6165 6170 6175 6180 6185 6190 6195 6200 6205 6210 6215 6220 6225 6230 6235 6240 6245 6250 6255 6260 6265 6270 6275 6280 6285 6290 6295 6300 6305 6310 6315 6320 6325 6330 6335 6340 6345 6350 6355 6360 6365 6370 6375 6380 6385 6390 6395 6400 6405 6410 6415 6420 6425 6430 6435 6440 6445 6450 6455 6460 6465 6470 6475 6480 6485 6490 6495 6500 6505 6510 6515 6520 6525 6530 6535 6540 6545 6550 6555 6560 6565 6570 6575 6580 6585 6590 6595 6600 6605 6610 6615 6620 6625 6630 6635 6640 6645 6650 6655 6660 6665 6670 6675 6680 6685 6690 6695 6700 6705 6710 6715 6720 6725 6730 6735 6740 6745 6750 6755 6760 6765 6770 6775 6780 6785 6790 6795 6800 6805 6810 6815 6820 6825 6830 6835 6840 6845 6850 6855 6860 6865 6870 6875 6880 6885 6890 6895 6900 6905 6910 6915 6920 6925 6930 6935 6940 6945 6950 6955 6960 6965 6970 6975 6980 6985 6990 6995 7000 7005 7010 7015 7020 7025 7030 7035 7040 7045 7050 7055 7060 7065 7070 7075 7080 7085 7090 7095 7100 7105 7110 7115 7120 7125 7130 7135 7140 7145 7150 7155 7160 7165 7170 7175 7180 7185 7190 7195 7200 7205 7210 7215 7220 7225 7230 7235 7240 7245 7250 7255 7260 7265 7270 7275 7280 7285 7290 7295 7300 7305 7310 7315 7320 7325 7330 7335 7340 7345 7350 7355 7360 7365 7370 7375 7380 7385 7390 7395 7400 7405 7410 7415 7420 7425 7430 7435 7440 7445 7450 7455 7460 7465 7470 7475 7480 7485 7490 7495 7500 7505 7510 7515 7520 7525 7530 7535 7540 7545 7550 7555 7560 7565 7570 7575 7580 7585 7590 7595 7600 7605 7610 7615 7620 7625 7630 7635 7640 7645 7650 7655 7660 7665 7670 7675 7680 7685 7690 7695 7700 7705 7710 7715 7720 7725 7730 7735 7740 7745 7750 7755 7760 7765 7770 7775 7780 7785 7790 7795 7800 7805 7810 7815 7820 7825 7830 7835 7840 7845 7850 7855 7860 7865 7870 7875 7880 7885 7890 7895 7900 7905 7910 7915 7920 7925 7930 7935 7940 7945 7950 7955 7960 7965 7970 7975 7980 7985 7990 7995 8000 8005 8010 8015 8020 8025 8030 8035 8040 8045 8050 8055 8060 8065 8070 8075 8080 8085 8090 8095 8100 8105 8110 8115 8120 8125 8130 8135 8140 8145 8150 8155 8160 8165 8170 8175 8180 8185 8190 8195 8200 8205 8210 8215 8220 8225 8230 8235 8240 8245 8250 8255 8260 8265 8270 8275 8280 8285 8290 8295 8300 8305 8310 8315 8320 8325 8330 8335 8340 8345 8350 8355 8360 8365 8370 8375 8380 8385 8390 8395 8400 8405 8410 8415 8420 8425 8430 8435 8440 8445 8450 8455 8460 8465 8470 8475 8480 8485 8490 8495 8500 8505 8510 8515 8520 8525 8530 8535 8540 8545 8550 8555 8560 8565 8570 8575 8580 8585 8590 8595 8600 8605 8610 8615 8620 8625 8630 8635 8640 8645 8650 8655 8660 8665 8670 8675 8680 8685 8690 8695 8700 8705 8710 8715 8720 8725 8730 8735 8740 8745 8750 8755 8760 8765 8770 8775 8780 8785 8790 8795 8800 8805 8810 8815 8820 8825 8830 8835 8840 8845 8850 8855 8860 8865 8870 8875 8880 8885 8890 8895 8900 8905 8910 8915 8920

voreingestellte Dateipfade, Spracheinstellungen, Menükonfigurationen und sonstige Benutzerpräferenzen. Diese Einstellungen werden den aufgerufenen Anwendungsprogramm 46 zugänglich gemacht, so dass der Benutzer immer mit der von ihm gewünschten Programmkonfiguration arbeitet. Dies gilt auch dann, wenn der Benutzer sein Benutzermodul 12 mit einem neuen oder anderen Mobilgerät 10 verbindet.

[0036] Bei hinreichender Standardisierung der Anwendungsprogrammierungsschnittstellen (APIs = application programming interfaces), wie sie beispielsweise durch Verwendung der Programmiersprache Java® mittelfristig zu erwarten ist, kann damit ein ASP-Anbieter für jeden Benutzer maßgeschneiderte und von dem benutzten Mobilgerät 10 unabhängige Anwendungsprogrammdienste anbieten. Überdies wird ein hohes Sicherheitsniveau erreicht, da sämtliche Anwendungsprogramme 46 nur bei Vorhandensein des Benutzermoduls 12 und nach Kennworteingabe aufrufbar sind. Um einen Missbrauch bei einem Diebstahl des Mobilgeräts 10 in eingeschaltetem Zustand (nach der Kennworteingabe durch den Benutzer) zu verhindern, kann vorgesehen sein, dass nach einer Unterbrechung der Benutzeraktivität für eine vorbestimmte Dauer wieder eine Kennworteingabe angefordert wird, wie dies beispielsweise bei Bildschirmschonern für stationäre Bürocomputer bereits an sich bekannt ist.

[0037] In dem bisher beschriebenen Ausführungsbeispiel wurde als kleinste Einheit für den Autorisierungsmechanismus und gegebenenfalls den Ladevorgang über die Luftschnittstelle 16 ein Anwendungsprogramm 46 angesehen. Abhängig von der eingesetzten Programmiertechnologie kann jedoch auch ein feineres Granularitätsniveau verwendet werden. Es können sich also die Konfigurationsdaten 62 beispielsweise auf die Berechtigung des Benutzers zum Ausführen einzelner Programmfunctionen oder einzelner Programm-Module beziehen, und diese Programmfunctionen oder Programm-Module können bei Bedarf einzeln über die Luftschnittstelle 16 geladen werden. Durch diese Vorgehensweise werden erstens lange Ladezeiten vermieden, und zweitens kann eine noch genauere Einstellung auf die Benutzerpräferenzen erfolgen. Auch bei der Aktualisierung von Anwendungsprogrammen 46 über die Luftschnittstelle 16 werden vorzugsweise nur solche Programm-Module übertragen, die sich gegenüber der bereits im Mobilgerät 10 befindlichen Version tatsächlich verändert haben.

[0038] Die von den Anwendungsprogrammen 46 bearbeiteten Nutzdaten 48 sind im Gerätespeicher 38 entweder vollständig oder zumindest teilweise in verschlüsselter Form abgelegt. Beispielsweise kann dem Benutzer ein Dateisystem zur Speicherung der Nutzdaten 48 bereitgestellt werden, bei dem einzelne Ordner oder einzelne Laufwerke wahlweise für eine verschlüsselte oder unverschlüsselte Datenspeicherung eingestellt werden können. Eine ähnliche Funktionalität für stationäre Bürocomputer ohne Einsatz eines Benutzermoduls ist bereits durch das Produkt PGPdisk® des Herstellers Network Associates, Inc., bekannt.

[0039] Wenn ein Anwendungsprogramm 46 Nutzdaten 48 in einem zur Verschlüsselung vorgesehenen Bereich des Dateisystems speichern möchte, werden diese Daten von der Prozessoreinheit 32 über die Schnittstelle 14 an das Benutzermodul 12 übertragen. Die Prozessoreinheit 50 des Benutzermoduls 12 führt die Verschlüsselungsfunktion 64 aus, wobei der in den Schlüsseldaten 60 enthaltene öffentliche Schlüssel 70 herangezogen wird. Die verschlüsselten Nutzdaten 48 werden über die Schnittstelle 14 und die Prozessoreinheit 32 in den Gerätespeicher 38 geschrieben.

[0040] Der Zugriff auf verschlüsselt abgelegte Nutzdaten 48 erfolgt entsprechend. Auch hier führt die Prozessoreinheit

50 des Benutzermoduls 12 die eigentliche Entschlüsselung unter Verwendung der Entschlüsselungsfunktion 66 und des privaten Schlüssels 72 aus. Vorab fordert die Prozessoreinheit 50 jedoch eine Kennworteingabe vom Benutzer an. Erst wenn das korrekte Kennwort (passphrase) auf der Tastatur 36 eingegeben wurde (oder eine sonstige biometrische Identifizierung des Benutzers korrekt durchgeführt wurde), wird der Entschlüsselungsvorgang freigegeben.

10 [0041] Im hier beschriebenen Ausführungsbeispiel wird die Ver- und Entschlüsselung nach einem asymmetrischen RSA-Verfahren durchgeführt. In Ausführungsalternativen sind dagegen andere asymmetrische oder symmetrische Ver- und Entschlüsselungsverfahren oder Mischformen davon, z. B. symmetrische Verschlüsselung unter Verwendung eines asymmetrisch verschlüsselten Schlüssels, vorgesehen. Bei symmetrischen Verfahren braucht nicht zwischen dem öffentlichen Schlüssel 70 und dem privaten Schlüssel 72 unterschieden zu werden.

15 [0042] Insgesamt wird durch die hier vorgeschlagene Technik sichergestellt, dass die verschlüsselten Nutzdaten 48 nur dann ausgelesen werden können, wenn das Benutzermodul 12 des berechtigten Benutzers an die Schnittstelle 14 angeschlossen ist und der Benutzer sich, z. B. mittels der 20 passphrase, korrekt identifiziert hat.

25 [0043] Im vorliegenden Ausführungsbeispiel wird der gesamte Ver- und Entschlüsselungsprozess von der Prozessoreinheit 50 des Benutzermoduls 12 durchgeführt, wobei die Schlüsseldaten 60 niemals das Benutzermodul 12 verlassen. 30 Es sind jedoch auch Ausführungsalternativen vorgesehen, bei denen die Verschlüsselungsfunktion 64 und der öffentliche Schlüssel 70, der nicht geheimgehalten zu werden braucht, an das Mobilgerät 10 übergeben werden, so dass der Verschlüsselungsvorgang durch die in der Regel leistungsfähigere Prozessoreinheit 32 des Mobilgeräts 10 durchgeführt werden kann. Für den Entschlüsselungsvorgang kann in manchen Ausführungsalternativen ebenfalls die Prozessoreinheit 32 herangezogen werden, solange dadurch die Sicherheit des privaten Schlüssels 72 nicht kompromittiert wird.

35 [0044] Zur Erzeugung der Schlüsseldaten 60 wird im vorliegenden Ausführungsbeispiel die Schlüsselerzeugungsfunktion 68 verwendet, die ebenfalls von der Prozessoreinheit 50 des Benutzermoduls 12 ausgeführt wird. Auf an sich bekannte Weise berechnet dieses Programm ein Paar aus öffentlichem Schlüssel 70 und privatem Schlüssel 72. Durch diese Maßnahme wird besonders hohe Datensicherheit gewährleistet, weil der private Schlüssel 72 auch bei der Schlüsselerzeugung das Benutzermodul 12 nicht verlässt.

40 [0045] Das hier beschriebene Ausführungsbeispiel ist nicht auf einen einzigen verschlüsselten Bereich für die Nutzdaten 48 und nicht auf ein einziges Verschlüsselungsverfahren beschränkt. So kann beispielsweise – entsprechende Legitimierung durch die passphrase vorausgesetzt – ein verschlüsselter Bereich jederzeit deaktiviert und damit frei zugänglich gemacht werden. Auch eine erneute Verschlüsselung mit demselben oder einem anderen Benutzermodul 12 ist möglich. Es können auch mehrere verschlüsselte Bereiche, gegebenenfalls mit unterschiedlichen 45 Schlüsselpaaren und/oder in verschiedenen Größen, angelegt und verwaltet werden.

50 [0046] Insbesondere bei der vorliegenden Ausgestaltung, die einen ASP-Anbieter vorsieht, können die verschlüsselten Nutzdaten 48 zusätzlich zur Speicherung im Mobilgerät 10 auch über die Luftschnittstelle 16 zu einem Server des ASP-Anbieters übertragen und dort gespeichert werden. Eine Synchronisierung der beiderseitig gespeicherten Nutzdaten 48 kann bei jedem Schreibzugriff eines Anwendungs-

programms 46 oder beim Beenden einer Benutzersitzung oder auf ausdrückliche Anforderung des Benutzers erfolgen. Der Benutzer hat dann einerseits schnellen Zugriff auf die lokal gespeicherten Nutzdaten 48 und ist andererseits von dem verwendeten Mobilgerät 10 unabhängig, weil er die beim ASP-Anbieter gespeicherten Nutzdaten 48 auch mit jedem anderen Mobilgerät abrufen kann.

[0047] Ferner kann in manchen Ausgestaltungen vorgesehen sein, eine Schlüsselkomponente beim Netzbetreiber oder dem ASP-Anbieter zu belassen. Nach erfolgreicher Einbuchung des Mobilgeräts 10 in das Telekommunikationsnetz 18 wird diese Schlüsselkomponente über die Luftschnittstelle 16 übertragen, so dass der Netzbetreiber oder ASP-Anbieter die Kontrolle über bestimmte im Mobilgerät 10 gespeicherte Nutzdaten 48 mit dem Benutzer teilt.

Patentansprüche

1. Verfahren zum Speichern von und Zugreifen auf Nutzdaten (48) in einem Mobilgerät (10), insbesondere 20 einem Mobiltelefon oder einem persönlichen digitalen Assistenten, das einen Gerätespeicher (38) aufweist und das über eine Schnittstelle (14) mit einem Benutzermodul (12) verbunden ist, dadurch gekennzeichnet, dass

die Nutzdaten (48) im Gerätespeicher (38) des Mobilgeräts (10) zumindest teilweise in verschlüsselter Form gespeichert werden, und dass zumindest das Entschlüsseln der Nutzdaten (48) bei Zugriffs vorgängen unter Verwendung einer Entschlüsselungsfunktion (66) erfolgt, die durch das Benutzermodul (12) bereitgestellt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass ferner das Verschlüsseln der Nutzdaten (48) bei Speichervorgängen unter Verwendung einer Verschlüsselungsfunktion (64) erfolgt, die durch das Benutzermodul (12) bereitgestellt wird.

3. Verfahren nach Anspruch 1 und Anspruch 2, dadurch gekennzeichnet, dass das Benutzermodul (12) einen Modulspeicher (52) aufweist, in dem die von dem Benutzermodul (12) bereitgestellten Ver- und Entschlüsselungsfunktionen (64, 66) sowie von diesen Funktionen (64, 66) verwendete Schlüsseldaten (60) enthalten sind, und dass die Ver- und Entschlüsselungsfunktionen (64, 66) zumindest teilweise von einer Prozessoreinheit (50) des Benutzermoduls (12) ausgeführt werden.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass durch das Benutzermodul (12) mindestens eine Funktion (68) zum Erzeugen der Schlüsseldaten (60) und zum Schreiben der Schlüsseldaten (60) in den Modulspeicher (52) bereitgestellt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zumindest die Ausführung der Entschlüsselungsfunktion (66) durch ein Kennwort und/oder eine biometrische Prüfung geschützt ist.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das Mobilgerät (10) ein auch für Telekommunikationsfunktionen eingerichtetes Gerät ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Benutzermodul (12) ein auch zur Einbuchung in ein Telekommunikationsnetz (18) vorgesehenes Teilnehmeridentifikationsmodul ist.

8. Mobilgerät (10), insbesondere Mobiltelefon oder persönlicher digitaler Assistent, das einen Gerätespeicher (38) und eine Schnittstelle (14) zum Anschluss ei-

nes Benutzermoduls (12) aufweist, dadurch gekennzeichnet, dass

über die Schnittstelle (14) Ver- und Entschlüsselungsfunktionen (64, 66) des Benutzermoduls (12) aufrufbar sind, und dass

der Gerätespeicher (38) mindestens einen Bereich für verschlüsselte Nutzdaten (48) aufweist, der zum Beschreiben und Lesen unter Verwendung der Ver- und Entschlüsselungsfunktionen (64, 66) des Benutzermoduls (12) eingerichtet ist.

9. Benutzermodul (12), insbesondere Teilnehmeridentifikationsmodul für ein Telekommunikationsnetz (18), das dazu eingerichtet ist, in Zusammenwirken mit einem Mobilgerät (10) nach Anspruch 8 ein Verfahren nach einem der Ansprüche 1 bis 7 auszuführen.

10. Verfahren zum Speichern von und Zugreifen auf Konfigurationsdaten (62) sowie zum Ausführen mindestens eines Anwendungsprogramms (46) in einem Mobilgerät (10), insbesondere einem Mobiltelefon oder einem persönlichen digitalen Assistenten, das einen Gerätespeicher (38) für das Anwendungsprogramm (46) aufweist und das über eine Schnittstelle (14) mit einem Modulspeicher (52) aufweisenden Benutzermodul (12) verbunden ist, dadurch gekennzeichnet, dass

die Konfigurationsdaten (62) zumindest auch die Verfügbarkeit des Anwendungsprogramms (46) oder einzelner Funktionen davon betreffen, und dass die Konfigurationsdaten (62) in dem Modulspeicher (52) gespeichert sind und aus diesem ausgelesen werden, um zu bestimmen, ob bzw. in welchem Umfang das Anwendungsprogramm (46) ausgeführt wird.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass das Auslesen der Konfigurationsdaten (62) aus dem Modulspeicher (52) durch ein Kennwort und/oder eine biometrische Prüfung geschützt ist.

12. Verfahren nach Anspruch 10 oder Anspruch 11, dadurch gekennzeichnet, dass zumindest Teile des Anwendungsprogramms (46) entsprechend den Konfigurationsdaten (62) in den Gerätespeicher (38) geladen werden.

13. Verfahren nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet, dass das Mobilgerät (10) ein auch für Telekommunikationsfunktionen eingerichtetes Gerät ist.

14. Verfahren nach den Ansprüchen 12 und 13, dadurch gekennzeichnet, dass die Übertragung von zumindest Teilen des Anwendungsprogramms (46) in den Gerätespeicher (38) unter Verwendung mindestens einer der Telekommunikationsfunktionen des Mobilgeräts (10) erfolgt.

15. Verfahren nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, dass das Benutzermodul (12) ein auch zur Einbuchung in ein Telekommunikationsnetz (18) vorgesehenes Teilnehmeridentifikationsmodul ist.

16. Verfahren nach einem der Ansprüche 10 bis 15, ferner mit den Merkmalen des Verfahrens nach einem der Ansprüche 1 bis 5.

17. Mobilgerät (10), insbesondere Mobiltelefon oder persönlicher digitaler Assistent, das einen Gerätespeicher (38) für ein Anwendungsprogramm (46) aufweist und das über eine Schnittstelle (14) mit einem Modulspeicher (52) aufweisenden Benutzermodul (12) verbunden ist, dadurch gekennzeichnet, dass über die Schnittstelle (14) Konfigurationsdaten (62) aus dem Modulspeicher (52) auslesbar sind, die zumindest auch die Verfügbarkeit des Anwendungspro-

gramms (46) oder einzelner Funktionen davon betreffen, und dass das Mobilgerät (10) dazu eingerichtet ist, in Abhängigkeit von den aus dem Modulspeicher (52) ausgelesenen Konfigurationsdaten (62) zu bestimmen, ob bzw. in welchem Umfang das Anwendungsprogramm (46) ausgeführt wird.

18. Mobilgerät (10) nach Anspruch 17, das dazu eingerichtet ist, in Zusammenwirken mit einem Benutzermodul (12) ein Verfahren nach einem der Ansprüche 10 bis 16 auszuführen.

19. Benutzermodul (12), insbesondere Teilnehmeridentifikationsmodul für ein Telekommunikationsnetz (18), das dazu eingerichtet ist, in Zusammenwirken mit einem Mobilgerät (10) nach Anspruch 17 ein Verfahren nach einem der Ansprüche 10 bis 16 auszuführen.

Hierzu 1 Seite(n) Zeichnungen

20

25

30

35

40

45

50

55

60

65

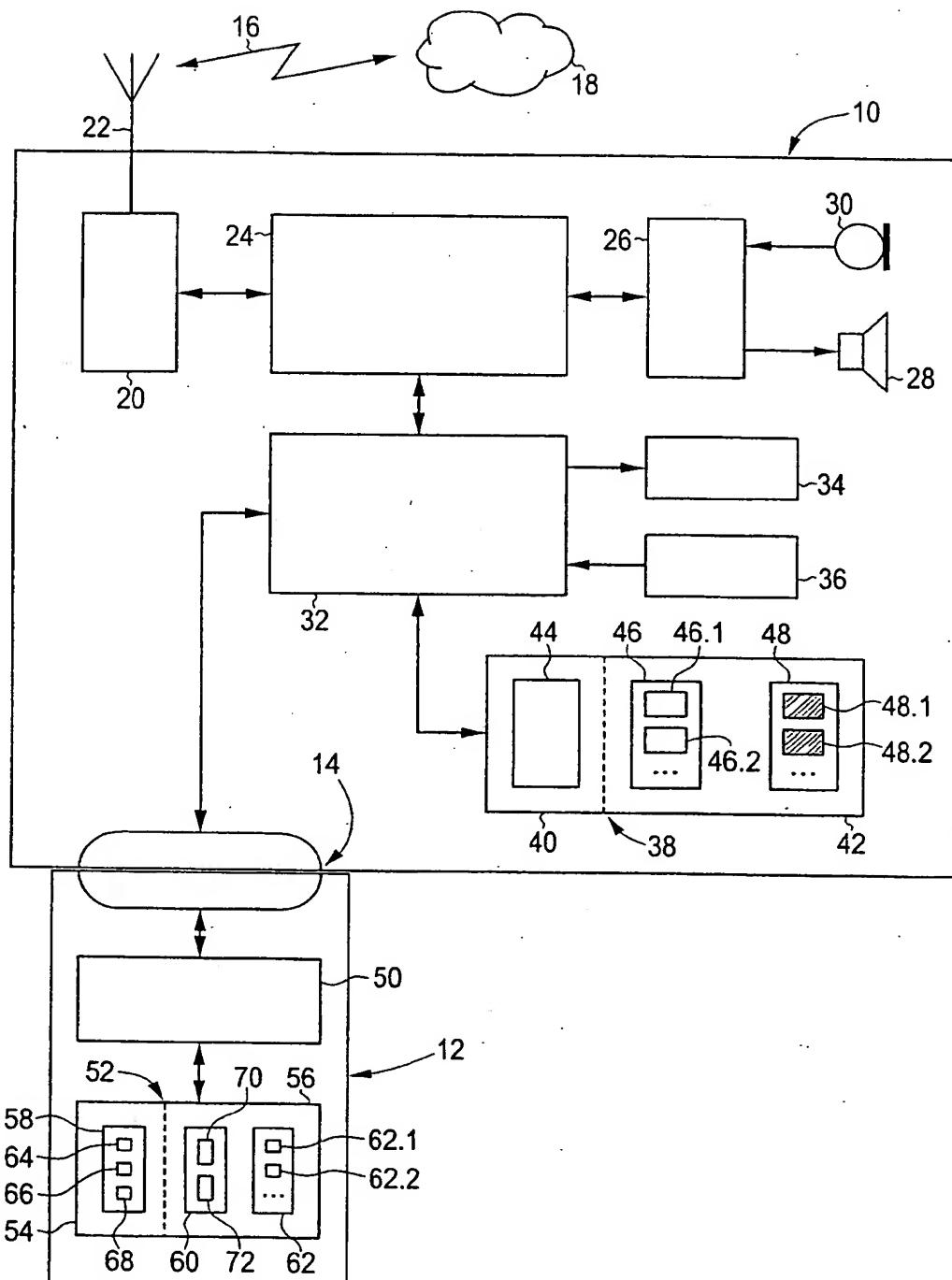


Fig. 1